United States Department of Agriculture
Marketing and Regulatory Programs
Animal and Plant Health Inspection Service

Directive **APHIS 3140.2** **5/26/2000**

APHIS ELECTRONIC MAIL SECURITY AND PRIVACY POLICY

1. PURPOSE

This Directive establishes:

a. The policy, foundation, rules and guidelines for the use, security, privacy, confidentiality, and integrity of electronic mail (e-mail) systems in APHIS.

b. The concept of reduced expectations of privacy that authorized users must accept when utilizing APHIS information resources for messaging purposes.

2. AUTHORITY AND REFERENCES

Foundation for the APHIS Information Systems Security (ISS) program is Directive 3140.1, dated 9/15/99. Applicable national policy requirements regarding ISS are stated primarily in Presidential Decision Directive 63, Critical Infrastructure Protection; the Computer Security Act of 1987 (Public Law (PL) 100-235); the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control; Appendix III of OMB Circular No. A-130, Management of Federal Information Resources; FED-STD-1037A, "An Electronic Means for Communicating Information; and the Electronic Communications Privacy Act (18 U.S.C. 2701). Taken together, these documents and others not cited prescribe establishing and maintaining a comprehensive Information Systems Security (ISS) program and set standards for using information systems, including electronic mail. Additionally, the United States Department of Agriculture (USDA) Office of Information Resources Management, Department Regulation 3140-1, USDA IRM Security Policy, applies, as do other USDA policies and requirements specifically related to e-mail Federal requirements related to protecting sensitive information, such as the Privacy Act of 1974 (PL 93-579, 5 U.S.C. 552a).

3. SCOPE

a. This Directive applies to all APHIS employees and contractors. It also applies to other Federal agencies, State and local governments, and authorized private organizations or individuals who use APHIS information systems and electronic messaging capabilities to accomplish an APHIS business function. All of the aforementioned are considered users and are included wherever the words “user” or “users” are referenced within this Directive.

b APHIS information systems (IS) covered by this Directive include all computer hardware software, and telecommunications that support APHIS electronic messaging systems, including electronic mail (e-mail) and facsimile (FAX) messages, transmitted and/or received by systems owned, operated, or funded by APHIS or those supplied for APHIS use by contractors.

c. This Directive does not apply to APHIS voice messaging systems.

4. POLICY

a. APHIS e-mail resources exist to enhance business capabilities and must be protected against waste, fraud, unauthorized use, or abuse. Use of electronic messaging in ways that violate ethical standards, deprive Americans of rightful value for their tax dollars, or embarrass this Agency will not be tolerated.

b. APHIS is committed to protecting sensitive information from accidental or Unauthorized release, transmission, display, or disclosure via electronic messaging. Sensitive information includes key Agency information (Privacy Act, contractual, etc.) as well as proprietary information of customers and cooperators. It is the responsibility of each APHIS Program/Business Unit to ensure that users are confident that their information is protected and that such confidence is justified.

c. All e-mail messages transmitted to or from or stored on APHIS computers are the property of APHIS. APHIS reserves the right to either randomly or systematically scan e-mail for improper materials. APHIS users have no right to expect their messages to remain private. Users who wish to ensure privacy of their communication should use means other than APHIS e-mail.

d. APHIS employees are permitted limited personal use of e-mail on an occasional basis, provided that the use involves minimal expense to the government, doesn’t interfere with official business, and take place during the employee’s personal time. Employees who have doubts about the meaning of “limited” or “occasional” should consult their supervisor. Employees must exercise good judgment in all use of e-mail. Official government business always takes precedence over personal use.

e. APHIS will comply with Federal and Departmental policies, regulations, and requirements on e-mail use and Information Systems Security.

5. RESPONSIBILITIES

a. The Chief Information Officer will:

(1) Approve and ensure implementation of e-mail security and privacy policies for the protection of APHIS information resources.

(2) Determine adequacy of security measures and accredit the APHIS e-mail system in accordance with Federal and USDA requirements.

(3) Ensure that procedures are in place to obtain consent for monitoring of e-mail systems, set forth in section 6., below.

(4) Ensure that system administrators are adequately trained and administrative procedures are developed, implemented, and monitored.

(5) Establish the Information Systems Security Program Manager (ISSPM) as the central point for providing guidance and coordination regarding e-mail security and privacy.

b. Deputy Directors of Program Units and heads of major business offices will:

(1) Ensure compliance with the provisions of this Directive. Through their Information Systems Security Managers (ISSM's) and other organizational security structure, implement and manage the provisions of this Directive throughout their organization.

(2) Ensure that users of e-mail systems are knowledgeable about the provisions of this Directive and that Unit ISSM's have the training and authority to promptly identify, investigate, and help rectify any violations of this Directive.

(3) Enforce policies and procedures to govern unauthorized material in e-mail messages.

(4) Ensure that the names of employees who leave the Unit are provided to the ISSM or Customer Service as possible prior to separation, but not later than 48 hours after the separation date. Users who are being removed for cause must have their e-mail access terminated immediately.

(5) Ensure that procedures are in place to obtain expressed consent, as defined in section 6., below, and records of expressed consent are maintained by the Unit ISSM or subordinate Information Systems Security Officers (ISSO's).

c. The ISSPM will:

(1) Be knowledgeable of and follow through on responsibilities identified in USDA ISS policies and procedures.

(2) Disseminate information concerning Federal and USDA e-mail security and privacy policies and developments.

(3) Develop, coordinate, implement, and maintain e-mail security and privacy policies for APHIS.

(4) Be involved in all investigations into misuse of e-mail systems.

(5) Ensure that a security plan has been prepared or updated to protect e-mail systems and that such systems are accredited in accordance with Federal and USDA requirements.

d. Unit Information Systems Security Managers (ISSM's) will:

(1) Administer this Directive and monitor its compliance in their Unit.

(2) Ensure that training exists to make users aware of their responsibilities for e-mail use, privacy, and security.

(3) Assist in promptly identifying, investigating, and helping rectify violations of this Directive.

(4) Ensure processes (or oversee those actions) to ensure that user identifications are disabled or deleted when employees (including contractors) depart the Unit and that other appropriate actions are taken to protect Agency e-mail records and access.

(5) Obtain and file (or oversee those actions) records of expressed consent for all users in their area of responsibility, including contractor personnel, in accordance with section 5., above.

e. Each APHIS employee who uses Agency e-mail must:

(1) Comply with this Directive and other ISS policies.

(2) Access (or attempt to access) only the e-mail account and messages which they have been authorized. Monitoring or accessing others' e-mail messages without their expressed consent is prohibited, except as noted in section 6., below.

(3) Take the necessary precautions to secure e-mail access from unauthorized users. Each employee is accountable for actions taken using their e-mail identification. Each employee:

(a) Must implement and maintain password protection for e-mail access.

1 Use effective passwords (not trivial, of personal significance, or easily guessed or deduced) and protect them properly (not post passwords, put them in automated script files, or program them as a function key).

2 Do not share passwords with others except to appropriate personnel in the course of a security investigation.

3 If mission requirements dictate that you provide others to access to your e-mail, use mail forwarding or set your user preferences to use other mechanisms that do not require you to share your e-mail password.

(b) Must change default passwords immediately, when receiving an e-mail account and password for the first time.

(c) Should change e-mail passwords at least quarterly.

(d) Should set e-mail preferences to lock access (which requires entering the e-mail password) after no more than five minutes of inactivity.

(4) Remain alert to the high potential for computer viruses and similar hostile computer programs that can be transmitted via e-mail. Users must use the greatest degree of caution to avoid malicious "logic bombs" that could seriously disrupt APHIS operations. Scan all e-mail message attachments, using up-to-date antivirus software.

(5) Treat unusual e-mail messages as they would unusual parcels. While attachments to e-mail messages or the messages themselves can be scanned for computer viruses or other hostile code, not all dangerous contents can be prevented or detected. The ingenuity or sophistication of an attacker combined with the gullibility of the recipient can result in hidden or dangerous encrypted content. Often it is best just to delete a message without opening it, if the user is unsure of the sender or the purpose of the message.

(6) Understand that sending an e-mail from an Agency/Unit mailbox or address is like sending a letter on official letterhead and may be interpreted as APHIS endorsement or policy.

(7) Maintain up-to-date e-mail distribution lists to ensure that only authorized

users receive e-mail via distribution lists.

(8) Protect sensitive and proprietary information. Users must:

(a) Refrain from sending nonpublic information to non-USDA addresses, except for authorized contractors/cooperators or other Federal agencies.

(b) Protect commercial proprietary information in accordance with the conditions under which it is purchased, provided or used.

(c) Prevent eavesdropping of sensitive e-mail by using available encryption.

(d) Use encryption, when available, to send sensitive FAX documents.

(9) Refrain from using e-mail and other electronic messaging systems for purposes that violate ethical standards. That includes harassment, sending sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth.

(10) Remember that e-mail accidents can have negative consequences for themselves and APHIS. Examples of accidents include:

(a) E-mail can be sent instantly to numerous destinations with no hope of retrieval. Messages can be misrouted by a single keystroke or click of a mouse. E-mail messages may be archived for years and result in damage or embarrassment months or years later.

(b) E-mail folders and directories can grow until the system crashes or system performance is impacted.

(c) Errors in e-mail lists can flood addresses with numerous errors or unwanted messages. Information may be sent to the wrong addressees.

(11) Logoff/logout of their e-mail sessions whenever leaving workstations for an extended period, including meetings, fire drills, and at the end of the day. (In a genuine emergency, users are not required to logoff/logout; protection of human life is paramount.)

(12) Sign a consent statement before being allowed accessing to the APHIS e-mail system. The statement will declare that the signer accepts responsibility for use of the system and their password and consents to

monitoring, according to the conditions of this Directive. This statement may be incorporated in a general user's security agreement.

(13) Report violations of this Directive to their ISSO or ISSM.

f. System managers/administrators and e-mail administrators will:

(1) Be responsible for supporting actions that help ensure compliance with this Directive, including ensuring that appropriate system security features are activated.

(2) Provide the ISSPM and Unit ISSM's with audit trails, system logs, and other information to assist with enforcement of this Directive and investigations into violations.

(3) Disable or delete user-ID's when notified that employees are leaving APHIS. Help arrange for transfer of files from departing employees to the supervisor or other designated personnel.

(4) Implement established technical safeguards (e.g., automatic logout/logoff features, audit trails, etc.) for e-mail systems, when feasible.

g. USDA Contracting Officers and Procurement Officials will:

(1) Ensure that procurement and contract documents clearly include the terms and conditions of this Directive, as appropriate.

(2) Ensure that contractors have signed security agreements relating to the terms and conditions of this Directive and that copies of the forms are maintained for later use, if needed.

(3) Assist the ISSPM in the investigation and information gathering of alleged violations of this Directive by contractor personnel.

(4) Ensure that the appropriate ISSM and/or systems managers or administrators are notified of departing or terminated contractors.

6. E-MAIL SYSTEM ADMINISTRATION

a. This Directive establishes APHIS “Rules of the System” for e-mail, as defined in Office of Management and Budget (OMB) Circular A-130, concerning the use and security of the e-mail and electronic messaging system.

b. E-mail and other electronic message systems are categorized as General Support Systems (GSS) and are therefore designated “sensitive” according to the requirements of the Computer Security Act of 1987; they will be accredited accordingly and technical security measures must be documented in the security plan for the system.

c. User identifications (user ID’s) should be assigned to specific individuals, readily identifiable for accountability purposes. User ID’s should be assigned by name rather than position (such as "Director") or other generic descriptor. When mission requirements demand use of generic ID’s, they should be restricted to “receive mode” only. All e-mail message sent from APHIS must be from a specifically identifiable individual.

d. Use of “visitor,” “guest,” “public,” “customer,” “anonymous,” or other unidentifiable entity is prohibited on APHIS e-mail systems. E-mail systems must also have vendor default or generic user-ID’s disabled or deleted.

e. Applicable system "patches" must be expeditiously applied to minimize the risk of outsiders exploiting known technical weaknesses.

f. System administrators and other personnel with special system level access privileges are prohibited from reading the e-mail of others except in pursuit of legitimate governmental purposes. These personnel must only reveal or act upon messages related to the problem at hand and not use assigned duties as a justification to simply browse employee files. Legitimate governmental purposes include:

(1) Performing troubleshooting and problem resolution, user assistance, debugging, system maintenance, risk mitigation, restoration procedures, and similar functions.

(2) Obtaining information in order to ensure continued operational capabilities.

(3) Assisting in retrieving a document for compelling business need. This will be done only upon written authorization from the ISSPM or Unit ISSM.

(4) Assisting with a documented investigative function by the APHIS Office of Inspector General (OIG) or law enforcement organization (e.g., Federal Bureau of Investigation, Drug Enforcement Agency, or Federal Protective

Service), or similar entity without prior notification of the user.

(5) Direction in writing by an employee relations specialist in response to a complaint of misuse, threats, or harassment.

(6) Investigating unwanted, unsolicited (junk e-mail or junk FAX), or offensive messages received by APHIS employees.

g. Monitoring e-mail.

(1) Warnings and notices.

(a) Prior to permitting access, all APHIS networked systems must display the following (or similar) warning banner: "All USDA/APHIS telecommunications and automated information systems and related equipment are for the communication, transmission, processing, and storage of U. S. Government information. These systems are subject to monitoring to ensure proper functioning, and to protect against improper or unauthorized use or access, and to verify the presence or performance of applicable security features and procedures, and for like purposes. Such monitoring may result in the acquisition, recording and analysis of data being communicated, transmitted, processed or stored in this system by any user. If monitoring reveals criminal activity, such evidence may be reported to law enforcement personnel. ANYONE USING A USDA/APHIS SYSTEM OR SYSTEM ACCESSED THROUGH A USDA/APHIS SYSTEM CONSENTS TO SUCH MONITORING."

(b) Electronic messaging systems must prohibit the display of "Welcome" messages or system identification messages until after the user has acknowledged the warning banner (by a keystroke or similar means) and has successfully logged into the system.

(c) APHIS Program/Business Units will ensure that each user signs a consent statement before accessing the e-mail system. By signing the statement, users accept responsibility for use and consent to monitoring according to the conditions of this Directive. That statement may be an APHISwide form or one specially developed by the Unit.

(d) Each APHIS Program/Business Unit must, when employing contractors or outsourcing, ensure that appropriate and binding nondisclosure forms are completed by all contractors performing e-mail, FAX, and FAX server system administrator/manager functions.

(2) Limitations on e-mail browsing and system monitoring:

(a) Unauthorized access or casual browsing of others' e-mail messages messages is strictly prohibited.

(b) A supervisor may access and read the electronic mail of a subordinate only:

1 With specific written approval of that employee.

2 In case of compelling business need, when the search is needed for an emergency but non-investigatory work-related purpose, such as to retrieve a time-critical document attached to the absent employee’s e- mail. In such cases the supervisor will request assistance (preferably in writing) from the Unit ISSM or the APHIS ISSPM. The supervisor must also promptly notify the employee of the action taken. Supervisors must make a good-faith effort to identify the specific document(s) needed and not use compelling need as a justification to simply browse employee files.

3 In the course of an approved investigation or to work with Human Resources, RMSES, or a law enforcement organization on investigatory or disciplinary actions.

(c) Supervisors may be given routine access to e-mail messages of former employees. The involvement of Human Resources, RMSES, or ISS personnel is not necessary for this action.

(3) Deleted e-mail messages are covered by this Directive and are subject to the same restrictions on browsing and retrieval. To eliminate retention of or access to unwanted messages, users should institute the procedures necessary to empty the “Recycle Bin” “TRASHCAN,” or “WASTEBASKET” at regular intervals.

h. Investigations.

(1) Supervisors or system administrators who suspect misuse of APHIS e-mail may request an investigation through the APHIS Resource Management Systems and Evaluation Staff (RMSES), who will coordinate with Human Resources and the ISSPM. Supervisors may request an investigation when there are reasonable grounds for suspecting that the electronic mail will produce evidence that an employee has engaged in work-related misconduct. Approved investigations will be documented and documentation retained by the RMSES, in coordination with the ISSPM. Disciplinary measures will be decided by the supervisor, in coordination with RMSES and Human Resources.

(2) The “Reasonableness Standard” will be applied when investigating misuse of electronic messaging and the development of electronic messaging policies by APHIS Program/Business Units. The Reasonableness Standard is a set of court-issued guidelines that should be applied whenever an e-mail search is conducted to ensure that the individual’s rights are not violated and that the government official is not required to get a search warrant each time it becomes necessary to enter an employee’s desk or files (both paper and electronic). The Reasonableness Standard asks: “Was the intrusion justified at its inception?” and “Was the search, as actually conducted, reasonable in its scope?”

i. FAX machines and servers are defined as electronic messaging devices and are within the scope of this regulation. System Administrators managing FAX servers will provide the same protections to FAX servers and messages as e-mail.

(1) FAX servers should be placed in areas where they can be regularly monitored for misuse.

(2) APHIS FAXes used to send and receive sensitive information must be protected from unauthorized or illegal use by implementing or activating security features that are available, including encryption, to protect incoming and outgoing facsimile transmissions.

j. All e-mail messages that meet the definition of official records (under the Federal Records Act will be preserved according to law. Theft, falsification, mutilation, or unauthorized disposition of official records is prohibited by law and subject to penalty. Contact the APHIS Records Manager for further information.

7. EXCEPTIONS

a. Exceptions that reduce the requirements of this Directive may be approved only in writing by the CIO or the APHIS Administrator.

b. Each Program/Business Unit is authorized to develop and implement policies and procedures, which may (based on risk assessment, mission, legislative mandate, or information sensitivity) be more stringent or specific than those documented in this Directive.

8. COMPLIANCE AND SANCTIONS

All personnel who use APHIS e-mail and other APHIS information resources are individually and personally responsible for complying with this Directive, as well as with the procedures and practices developed in support of this Directive. Willful failure to comply may result in punishment, including dismissal, under the Computer Fraud and Abuse Act. Management failure to comply with privacy protections and implement privacy security standards can result in civil liability.

9. INQUIRIES

a. Direct inquiries or requests for changes to this Directive to the APHIS Information Systems Security Program Manager, 555 Howes Street, Fort Collins, CO 80521 or call 970-490-7814.

b. Copies of current APHIS directives can be accessed on the Internet at ***www.aphis.usda.gov/library***.

APHIS Chief Information Officer